AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

I, Special Agent Alejandro Urzua, being duly sworn, depose and state as follows:

AFFIANT'S BACKGROUND

1. That I, Alejandro Urzua, am a Special Agent with the Drug Enforcement Administration (DEA) and have been so employed since January 2022. I am a 16-year veteran of law enforcement and have been employed as a federal law enforcement officer for over 16-years. I am currently assigned to the DEA Tucson District Office in the Phoenix Field Division to investigate violations of the Controlled Substance Act.
2. I attended DEA Basic Agent Training in 2022 at the DEA Training Academy in Quantico, Virginia. The 17-week training course included classes on the investigation, detection and identification of Controlled Substance Act violations; the methods of operation of Drug Trafficking Organizations (DTOs); and the practices for interviewing witnesses, cooperating individuals, and others who may have knowledge regarding controlled substances.
3. Previous to employment with the DEA, your Affiant was employed as a federal agent with the United States Border Patrol (USBP) from 2007 until 2022. I completed the USBP Academy based at the Federal Law Enforcement Training Center (FLETC) in Artesia, New Mexico and received approximately 12 weeks of specialized training at FLETC. As a Border Patrol Agent, I was assigned to intelligence units where I participated in numerous human smuggling and narcotics investigations. I also worked with different federal, state and local agencies to assist in those investigations.

4. I have received extensive field training of narcotics and the methods and practices of DTO's. I have attended numerous law enforcement courses and have been trained to observe and detect the common actions of narcotics traffickers and their co-conspirators in overt acts to further the commission of their crimes. I have taken part in numerous criminal investigations which have led to the successful arrests and convictions of those being investigated.

5. As part of this investigation, I have consulted with other agents and analysts assigned to the DEA Tucson District Office. Specific to this affidavit, I have relied upon the work of James Hart, an Intelligence Research Specialist with the Drug Enforcement Administration, currently assigned to the DEA Tucson District Office, Intelligence Group 2. Mr. Hart has been in Finance and Intelligence positions for seven years. Prior to this position, Mr. Hart was a Tucson Police Officer/ Detective from May 1994 to August of 2023.

6. I have participated in the execution of search and seizure warrants involving electronic evidence and have been involved in investigations of narcotics-related crimes. I have conducted investigations concerning the unlawful distribution of illegal narcotics, possession with intent to distribute controlled substances, importation of illegal narcotics, use of communications to conduct illegal narcotics transactions, maintaining places for purposes of manufacturing, distributing, or using controlled substances, and conspiracies to commit these offenses, in violation of Title 21, United States Code, Sections 841, 843, 846, 952, and 963. Based upon this experience, and conversations with other investigators and detectives with numerous years of experience, I have also

become well-versed in the methodology utilized in illegal narcotics trafficking, the specific type of language used by illegal narcotics traffickers, and the unique patterns employed by narcotics organizations. I have also conducted physical surveillances and electronic surveillances. Additionally, I have arrested individuals for various drug violations and have spoken with several drug dealers, drug users, and informants concerning the methods and practices of drug traffickers. I have had many discussions with other experienced law enforcement officers and have conducted, and been present at, many interviews of self-admitted narcotics traffickers and cooperating defendants concerning how drug traffickers and money launderers operate.

7. I know that drug traffickers often hold proceeds traceable to their drug-trafficking activities in the form of United States currency, funds in bank accounts, high-value personal property items, and real property. But I also know that drug traffickers are now increasingly holding drug-trafficking proceeds in virtual currency or cryptocurrency. Based on my training, research, education, and experience, I am familiar with the relevant terms and definitions set forth in the section titled "Background on the Illicit Sale of Steroids on the Open Web, Darknet and the Use of Cryptocurrency" below. I know that cryptocurrencies are different from traditional currencies in that cryptocurrencies are not issued by or backed by any government. In addition, cryptocurrency accounts and wallets are different from traditional bank accounts in that these accounts are held in digital format in one of any number of various types of digital wallets or exchanges. Likewise, cryptocurrency is accessible only by the account holder or someone who has access to the account password or account

"recovery seed[1]," a mnemonic passphrase made up of a series of random words, or in some circumstances, by the company hosting the virtual wallet containing the cryptocurrency. Account holders have the ability to send and receive cryptocurrency using a unique and complex wallet address, often referred to as the private key.

8. Because I am submitting this affidavit for the limited purpose of establishing probable cause for the requested seizure warrants, I have not included in this affidavit every detail I know about this investigation. Rather, I have included only the information necessary to establish probable cause for the requested seizure warrants.

9. The facts set forth in this affidavit are based on my personal knowledge, including what I have learned through my training and experience as a law enforcement officer, my review of documents and other records obtained in the course of this investigation, and information I have obtained in the course of this investigation from witnesses having personal knowledge of the events and circumstances described herein and other law enforcement officers, all of whom I believe to be truthful and reliable.

INTRODUCTION

10. I submit this affidavit in support of applications for a warrant to seize all cryptocurrency and fiat currency associated with certain digital wallets owned and controlled by Rebekah Cheri Dietrich (DIETRICH), Jorge Olivarria (OLIVARRIA) and Carlos

[1] A "recovery seed" is a mnemonic passphrase made up of 12 or 24 random words. It acts as a backup, ensuring that the wallet's funds can always be accessed. Anyone with the "recovery seed" can gain access to and control the wallet's funds. The recovery seed is a root key, sometimes referred to as a root seed, recovery seed, or mnemonic seed. A root key is a back-up key to the private key and allows a wallet owner to re-generate a new key pair for the corresponding wallet, offline and outside of the company or software that originally generated it. After re-generating the wallet with a root key, the possessor of the new wallet now has the ability to send and receive the value (in this example, cryptocurrency) associated with the original key pairs using the new private key created by the root key or "recovery seed."

Alberto Jimenez (JIMENEZ). DIETRICH, OLIVARRIA, and JIMENEZ make up a cell of the Charles GILBERT Drug Trafficking Organization (GILBERT DTO). GILBERT and DIETRICH reside at 7013 W Amarante, Tucson AZ (Amarante address) The wallets in question are specifically described as follows:[2]

a. Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com cryptocurrency exchange – Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com account and wallets associated with user ID 40415631, registered under the name of "REBEKAH CHERI DIETRICH" and using email address rebekahcheri@gmail.com. (Hereinafter, collectively referred to as "**Subject Wallet 1**").

b. Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com cryptocurrency exchange –Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com account and wallets associated with user ID 2933498, registered under the name of "JORGE OLIVARRIA" and using email address JORGEOLIVARRIA88@gmail.com. (Hereinafter, collectively referred to as "**Subject Wallet 2**").

c. Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com cryptocurrency exchange – Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com account and wallets associated with user ID 42226557 registered under the name of "CARLOS ALBERTO JIMENEZ" and using email address

[2] Identifying information about the subject wallet, such as the username and pin or the complete wallet recover seed, is redacted to protect the wallet from being accessed by the subject or anyone else, either before or after the warrant is executed.

carlosj578@gmail.com. (Hereinafter, collectively referred to as "**Subject Wallet 3**").

11. For the reasons set forth below, I submit that there is probable cause to believe that the funds contained in **Subject Wallet 1**, **Subject Wallet 2,** and **Subject Wallet 3** constitute or are derived from proceeds of drug trafficking and mail fraud, and constitute property involved in money laundering offenses, in violation 18 U.S.C. §§ 1956 and 1957, and therefore are subject to criminal forfeiture pursuant to 21 U.S.C. §853, and 18, U.S.C. §982(a)(1), and is subject to criminal seizure warrant pursuant to 21 U.S.C. §§853(e), 853(f), and 18 U.S.C. §982(b)(1).

Background on the Illicit Sale of Steroids on the Open Web, Darknet and the Use of Cryptocurrency and Cryptocurrency Mixers/Tumblers

12. The Open Web is the accumulated and indexed websites available without the use of password or anonymizing software. This is the internet we use on a regular business and where websites are reached by entering the web address or through a search engine. Illicit steroid use and sale are discussed on numerous online forums and online body building communities. In these forums users discuss websites where they are able to purchase illicit steroids and discuss the quality of products. By viewing these discussions, we are able to identify specific websites selling illicit steroid and diverted pharmaceuticals.

13. The "darknet" is a portion of the "Deep Web" of the internet,[3] where individuals must use anonymizing software or an application to access content and websites. The darknet is home to criminal marketplaces, also called "hidden services", where individuals can buy and sell illegal items, such as drugs, firearms, and other hazardous materials with greater anonymity than is possible on the traditional internet (sometimes called the "clear web" or simply the "web"). Darknet Marketplaces (DNMs) operate in a manner similar to clear-web commercial websites, such as Amazon and eBay, but they offer illegal items and they also use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to shield communications and transactions from interception and monitoring. Examples of such DNMs that offered illicit goods and services include Silk Road, AlphaBay, and Hansa, all of which have since been shut down by law enforcement.

14. On DNMs, vendors create and operate "vendor accounts" and customers create and use "customer accounts," just as legitimate vendors and customers do on clear-web marketplaces. Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a legitimate clear website. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate

[3] The Deep Web is the portion of the internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a DNM in exchange for cryptocurrency, while that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency.[4] Likewise, a person on the darknet could use different accounts to send and receive the same cryptocurrency. I know from training and experience that one of the reasons DNM vendors often have and use multiple vendor and customer accounts is to conceal from law enforcement both their identities and which accounts they own and control.

15. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the internet, distributed around the world, whose purpose is to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites

[4] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

are AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a Tor enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

16. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether.

17. Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object.

18. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries.

19. Generally, cryptocurrency is not issued by any government, bank, or company. Instead, cryptocurrency is generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[5] Cryptocurrency is not illegal in the United States.

[5] But some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

20. Bitcoin[6] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (*i.e.*, online companies that allow individuals to buy or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And although bitcoin transactions are not completely anonymous, bitcoin does allow users to transfer funds more anonymously than traditional financial transactions.

[6] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter "B") to label the protocol, software, and community, and "bitcoin" (with a lowercase letter "b") to label units of the cryptocurrency. That practice is adopted here.

21. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and then generate, store, or generate and store public and private keys used to send and receive cryptocurrency. A public key, or public address, is akin to a bank account number. A private key, or private address, is akin to a PIN number or password that allows a user to access and transfer value associated with the public address or key.

22. To conduct transactions on a blockchain, an individual must use the public address as well as the private key. A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of a public address's private key can authorize any transfers of cryptocurrency from that cryptocurrency public address to another cryptocurrency address.

23. Each private key and/or wallet can control multiple public addresses. These groupings of public addresses associated with one private key or wallet are referred to as address clusters. These linked addresses can be identified by investigators through co-spend and change transactions shown on the blockchain. A co-spend is a transaction in which two or more blockchain addresses send a balance to an additional blockchain address, which indicates that the multiple sending addresses are associated with the same wallet or private key. A change address is a blockchain address that receives the remainder of cryptocurrency sent to an additional address in a transaction. As the Bitcoin cryptocurrency protocol necessitates sending an address' entire balance in any

transaction, the amount not intended to be deposited is returned to the sender as change. These change addresses can be attributed to the sender's private key or wallet.

24. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is frequently used by individuals and organizations for criminal purposes, such as to pay for illegal goods and services – via, for example, hidden services websites operating on the Tor network.

25. Cryptocurrencies can also be used to engage in money laundering. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the DNMs.

26. A cryptocurrency user can store and access wallet software in a variety of forms, including via:

- a PC or laptop ("desktop wallet"),
- a mobile application on a smartphone or tablet ("mobile wallet"),
- an internet-based cloud storage provider ("online wallet"),
- an online account associated with a cryptocurrency exchange ("online account"),
- a tangible, external device, such as a USB thumb drive ("hardware wallet"), or
- printed public and private keys ("paper wallet").

Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (*e.g.*, smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB

thumb drive or other commercially available device designed to store cryptocurrency (*e.g.*, Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[7] with the public and private key embedded in the code. Paper wallet keys are not stored digitally.

27. Wallets can also be backed up via, for example, paper printouts, USB drives, or CDs. Wallets can be accessed through a password or a "recovery seed" or "mnemonic phrase," that is, random words strung together in a phrase.

28. Additional security safeguards for cryptocurrency wallets can include two-factor authorization, such as a password and a phrase. I know that individuals possessing cryptocurrencies often have safeguards in place to prevent their assets from hacking, unauthorized transfer, and/or law enforcement seizure.

29. Cryptocurrency "exchangers" and "exchanges" are individuals or companies that exchange or transmit bitcoin and other cryptocurrencies for other currencies, including U.S. dollars. According to Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) Guidance issued on March 18, 2013, and May 9, 2019, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses ("MSBs").[8] MSBs, including cryptocurrency exchanges, function as regulated businesses subject to the federal Bank

[7] A QR code is a matrix barcode that is a machine-readable optical label.

[8] *See* FinCEN Guidance FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019; FinCEN Guidance FIN-2013-G001, "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," March 18, 2013.

Secrecy Act ("BSA").[9] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (AML) regulations, "Know Your Customer" (KYC) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% of the amount exchanged, in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%.

30. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or

[9] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970).

password. Users can store, receive, and transfer cryptocurrencies via the application. But many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed, or on any digital or physical backup private key that the user creates. As a result, these wallet service companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet, described above, law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and then transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

31. As of December 30, 2024, one bitcoin is worth approximately $92,000 US Dollars (USD). But the value of bitcoin is volatile, and its value, to date, has been more volatile than that of widely accepted fiat currencies such as the U.S. dollar.

32. Cryptocurrency tumblers/mixers are a service used to obfuscate the source and destination of cryptocurrency transfers. These services take in transfers and break them into numerous smaller amounts, create multiple transaction chains and output the funds to the desired account. These services are designed to hamper the use of blockchain tracing used by law enforcement. By breaking up the funds and routing them through

multiple wallets prior to the ultimate destination the tracing of the funds becomes difficult if not impossible. These services charge an added fee for the process and are not used by typical users because of the added cost. Each transfer incurs a cost to the user. Several of these services have been identified and investigated by law enforcement as illicit money laundering services. As an example, the ChipMixer tumbler/mixer was shut down in a joint international investigation. ChipMixer is one of the mixers/tumblers used by the GILBERT DTO. The Wasabi mixer/tumbler ceased activity in June of 2024.

FACTS SUPPORTING FINDINGS OF PROBABLE CAUSE

33. In May 2022, the Drug Enforcement Administration (DEA) Tucson in conjunction with the United States Postal Inspection Service (USPIS) in Tucson, AZ identified an illicit steroid operation shipping parcels in Casa Grande, AZ, Coolidge, AZ, Phoenix AZ, and Tucson, AZ. The parcels were being shipped to locations across the United States (U.S.). Agents have been able to identify over 8,000 parcels shipped through the U.S. Postal Service attributable to this organization as of August 2024.

34. On January 10, 2025, United States Magistrate Judge Maria S. Aguilera signed seizure warrants for Subject Wallet 1, Subject Wallet 2, and Subject Wallet 3 held by Crypto.com exchange. Upon execution of said warrants on January 14, 2025, to Crypto.com exchange, law enforcement was notified that Crypto.com is a trade name and the legal name of the exchange that controls or holds **Subject Wallet 1, Subject Wallet 2,** and **Subject Wallet 3** is Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com cryptocurrency exchange – Foris Dax Inc**,** Foris Inc**.** and Foris

Services, Inc., doing business as (dba) Crypto.com. The following alleged facts support the seizure of said wallets using the correct legal names of said entity.

35. The parcels include a return address that is used on multiple labels created on the same day. Agents were able to identify common recipients receiving multiple parcels from different fraudulent return addresses.

36. On May 22, 2022, the USPIS intercepted a package being sent to a subject in the state of Washington. Agents contacted the subject who consented to opening the parcel. The parcel was found to contain vials labeled testosterone (a Schedule III Controlled Substance,) and Global Labs. Agents identified four prior parcels sent to this subject from Arizona. The subject stated he purchased the vials from the website PharmaHGH.net and paid using cryptocurrency. The subject sent the cryptocurrency to Bitcoin wallet 1AbXA7MhK6QAuGg6JQjcfaZ56 (1AbXa7M). A review of 1AbXa7M showed this wallet made multiple outbound transfers to the Wasabi cryptocurrency mixer/tumbler.

37. Agents reviewed PharmaHGH.net and observed numerous Schedule III controlled substances offered for sale (mostly steroids). The website also offered diverted pharmaceuticals such as those observed being smuggled into the U.S. from European countries such as Turkey. PharmaHGH.net accepts cryptocurrency for payment. The main source of payments is Bitcoin. A review was conducted of known PharmaHGH.net Bitcoin payment acceptance wallets. Twenty known Bitcoin payment acceptance wallets were reviewed from January 3, 2024, through October 21, 2024. During this period the known wallets received 3,589 inbound transfers. The total

amount transferred was approximately $807,081. This is an average of $225 per transfer. The injectables listed for sale on PharmaHGH.net range in price from $25 to $100. The oral products listed for sale on the site range in price from $35-$120. The domestic HGH listed for sale on the site ranged in price from $170-$200. The international HGH listed for sale on the site range in price from $110 to $340. The peptides listed for sale on the site range in price from $28-$57. The international pharmaceuticals for sale on the site range in price from $25-$265. Cryptocurrency payments made to PharmaHGH.net have been received by GILBERT DTO members and GILBERT has been observed shipping parcels containing steroids sold from this website. The investigation has revealed that the GILBERT DTO members utilize PharmaHGH.net to advertise the sale of steroids and other controlled substances and collect and receive cryptocurrency payments in their own individual wallets from PharmaHGH.net customers (**Subject Wallets 1-3**).

38. On August 10, 2023, law enforcement officers (LEOs) used this information, and obtained a federal search warrant for a suspicious parcel that was shipping from an address in Tucson, AZ, to a Mike Durazo in Surprise, AZ. This parcel was identified as having a fictitious name and the label had similar characteristics to labels on previously seized parcels, especially those containing steroids. From LEOs' training and experience, nearly all drug and drug proceed parcels bear tracking numbers allowing the sender and receiver to track the progress of the shipment from origination to destination and are also paid in cash or crypto to keep anonymity. On this occasion, the parcel contained a pre-paid label. Inside the parcel, LEOs located approximately

240 grams of suspected steroids. Lab analysis confirmed that the suspected steroids were indeed steroids, Schedule III controlled substances.

39. On August 18, 2023, LEOs again used the same information and obtained a federal search warrant for another suspicious parcel that was shipped on August 12, 2023, from an address in Tucson, AZ to a Michael Howard, in Tucson, AZ. This parcel was also identified as having a fictitious name and return address, and the label had similar characteristics to labels on previously seized parcels. LEOs also checked law enforcement databases and public records but found no records associating the sender with the listed address. Inside the parcel, LEOs located approximately 83 grams of suspected steroids.

40. On August 24, 2023, a subject was observed shipping parcels matching others shipped by this organization. Through open-source investigation the subject was identified as GILBERT. GILBERT's address was identified as 7013 W. Amarante, Tucson, AZ 85743.

41. On September 19, 2023, LEOs obtained a federal search warrant for another suspicious parcel with the same characteristics mailed on September 18, 2023, by this drug trafficking organization (DTO). That parcel contained 180 grams of suspected steroids. Lab analysis confirmed that the suspected steroids were indeed steroids, Schedule III controlled substances. Surveillance footage shows GILBERT mailing the parcels.

42. On October 18, 2023, agents conducted surveillance of GILBERT. During the surveillance GILBERT, was observed going to the post office located at 7959 N Thornydale, Tucson, AZ. GILBERT was observed entering the post office carrying a

brown bag. Agents identified parcels shipped by GILBERT and one parcel was intercepted. This parcel was turned over to the USPIS. A search warrant was obtained and this parcel was found to contain Testosterone Cypionate vials, a Trenbalone Enanthate vial, and Trenbolone Acetate vials. All vials were branded Global Labs. Lab tests of the vials showed the presence of steroids in the parcel, Schedule III controlled substances.

43. On October 25, 2023, surveillance was conducted on a secondary address determined by LEOs to be controlled by GILBERT at 291 W Byrd Ave, Coolidge, AZ (Coolidge address). GILBERT was observed on surveillance video gaining access to the property using keys for the front door. The Pinal County Assessor lists this address as a rental property. Agents also observed a subject later identified as Jorge OLIVARRIA exit the Coolidge residence on this date. OLIVARRIA was followed to the post office at 229 W Central Ave, Coolidge, AZ. OLIVARRIA was observed entering the post office with grocery bags. Agents identified 11 parcels mailed by OLIVARRIA. One of these parcels was intercepted by the USPIS. A search warrant was obtained for the parcel, and it was found to contain items labeled Testosterone Enanthate vials, Drostanolone vials, a Trenbolone vial, and a bag of Anastrozole pills (consistent with steroids). All products were labeled Global Labs. Although the items appear to be steroids, no lab reports are available for these items as of this writing.

44. On November 6, 2023, electronic surveillance showed Gilbert's truck going to the post office at 7959 N Thornydale, Tucson, AZ. Postal service business records showed 13

parcels matching the parcel shipping characteristics identified for this organization were mailed at that location.

45. On December 5, 2023, GILBERT was observed on electronic surveillance leaving the Byrd address, with a large reusable shopping bag. GILBERT was then observed on electronic surveillance going to the post office on Central Ave. in Coolidge, AZ. The USPIS interdicted one of the parcels matching the characteristics of this organization. A search warrant was obtained and this parcel was found to contain products labeled Testosterone Cypionate vials, a Testosterone Enanthate vial, Trenbolone vials, Dinabol capsules, and Anavar capsules. The products were branded Global Labs. Lab analysis revealed the suspected steroids were indeed steroids, Schedule III controlled substances.

46. On February 15, 2024, Gilbert was observed on electronic surveillance traveling to the post office located at 7959 N Thornydale, Tucson, AZ. The USPIS intercepted a parcel mailed at that location. A search warrant was obtained and the parcel was found to contain products labeled Testosterone Cypionate vial, Drostanolone Enanthate vial, Tadalafil capsules, Fluoxmesterone capsules, and vials of an unknown substance. With the exception of the three unknown vials the items were labeled Global Labs. Lab analysis revealed the suspected steroids were indeed steroids, Schedule III controlled substances.

47. On April 9, 2024, Agents conducted surveillance at the Amarante Dr. address, in Tucson, Arizona. GILBERT was observed exiting the neighborhood. GILBERT was followed to the post office located at 7959 N Thornydale Rd, Tucson, AZ. GILBERT

entered the post office carrying two packages. The USPIS interdicted one of the parcels matching the parcel shipping characteristics of this organization. A search warrant was obtained and this parcel was found to contain products labeled Testosterone Cypionate vials, Trenbolone vials, a Nandrolone Phenylpropionate vial and Masterolone capsules. The products were branded Global Labs. Lab analysis confirmed that the suspected steroids were indeed steroids, Schedule III controlled substances.

48. On May 6, 2024, agents observed GILBERT drove to his residence at 7013 W Amarante, Tucson, AZ, and met with OLIVARRIA. Agents observed OLIVARRIA walking away from GILBERT carrying two large rectangular shopping bags. OLIVARRIA left and drove to the post office located at 7959 N Thornydale, Tucson, Arizona. Agents observed OLIVARRIA enter the post office carrying a bag. Agents observed OLIVARRIA empty the bag into the drop box at the post office. Agents identified 19 parcels. The USPIS intercepted one of the parcels. A search warrant was obtained and the parcel was found to contain products labeled Testosterone Cypionate vials, Trenbolone Acetate vials, and Tadalafil capsules. Lab analysis confirmed that the suspected steroids were indeed steroids, Schedule III controlled substances.

49. On September 12, 2024, postal employees from the Cortaro U.S. Post Office in Tucson, Arizona notified a U.S. Postal Inspector that GILBERT had mailed suspicious packages that met the indicators of earlier packages mailed by him and some seized that contained steroids, a Schedule III controlled substance. On September 23, 2024, a federal search warrant was obtained to search one such parcel shipped to JIMENEZ in Florida. Inside the parcel were 310 grams of Oxazepam, a benzodiazepine, and Schedule IV controlled

substance as confirmed by a field test. On September 25, 2024, a U.S. Postal Inspectors observed video footage of GILBERT mail a parcel from the Cortaro U.S. Post Office to JIMENEZ in Orlando, Florida.

50. Cryptocurrency accounts were identified for GILBERT, DIETRICH, OLIVARRIA, and JIMENEZ via subpoenas and cryptocurrency tracing. In addition, a significant number of payments from PharmaHGH.net have been and are being deposited into **Subject Wallets 1-3**. Each of these individuals are believed to be steroid and illegal controlled substance distributors. JIMENEZ is based out of the state of Florida and based on the amount of funds sent to him through crypto exchanges by the other members of the GILBERT DTO he appears to have the role of drug distributor in the Southeast United States.

51. Three cryptocurrency accounts have been historically identified as GILBERT'S cryptocurrency wallets. The first GILBERT account or wallet was held in the Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com exchange and has since been dormant or inactive. The second GILBERT account or wallet was held in the Coinbase exchange, and it too is now dormant or inactive. The third GILBERT account is held by Kracken cryptocurrency exchange and is presently active and was seized on January 14, 2025, pursuant to a seizure warrant authorized by U.S. Magistrate Judge Maria S. Aguilera. The account identified in the Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com included the Bitcoin wallet 3P9GkFFmGxJr3K55gM3MaAmsL5bjBMvgcs (3P9GkFF). This older and now dormant wallet was first observed on the Bitcoin blockchain on July 21, 2020. The last

observed transaction occurred on February 4, 2023. This wallet was involved in a total of 112 transactions, 56 inbound and 56 outbound. The inbound total was $204,339. The outbound total was $191,801. A review of the inbound transactions showed the funds originated from the Wasabi and ChipMixer cryptocurrency tumblers (see paragraph 32 for more details). Deposits were observed from other un-hosted wallets. This account also had a debit card attached to it. This card was used to make debit withdrawals at First Hawaiian bank, Wells Fargo bank, Chase bank, and Great Western/ First Interstate bank. This card was also used for multiple payments to Arizona Kawasaki KTM Triumph (AZKKT). Payments were made to "MEDLABSUPPLY" with this card. "MEDLABSUPPLY" is a company that sells containers and vials that are commonly used to house and dispense liquid controlled substances such as steroids. Payments totaling $12,493.90 were made to Sheffield's Jewelers. The debit card was also used for everyday life pattern charges. Again, the funds contained in these wallets were cryptocurrency derived from sales from PharmaHGH.net and represent the proceeds of illegal drug sales.

52. The GILBERT account identified at the Coinbase exchange contained Bitcoin wallet 3CGDo9mCYTGW9W6tsogLmikpc2Vwpk39iP (3CGDo9m). This older and now dormant wallet first appeared on the Bitcoin blockchain on October 10, 2022. The last transaction for this wallet occurred on June 4, 2024. This wallet has been involved in a total of 186 transactions. There were 93 inbound and 93 outbound transactions. The inbound transactions totaled $556,102. The outbound transactions $556,382. A review of the inbound transactions for 3CGDo9m show transfers originating from the

ChipMixer, CryptoMixer and Wasabi cryptocurrency tumblers (see paragraph 32 for details). Other deposits were observed from another non-custodial (not assigned to a known user like S**ubject Wallets 1-3**) exchange based in the Czech Republic which receives deposits from PharmaHGH.net Bitcoin payment acceptance wallets. Deposits were also observed from other un-hosted wallets. This older now dormant wallet also had an associated debit card. Payments were observed to "MEDLABSUPPLY" and via PayPal on eight occasions. Med Lab Supply is a company that sells medical and laboratory supplies including empty capsules and vials easily used in the distribution of controlled substances like steroids. Payments were also observed to "AMZ*Capsule Supplies" on seven occasions. A payment to AZKKT was observed. Thirty withdrawals from this wallet were observed being transferred to First Interstate bank. The total of these transactions was $286,127.70.

53. A Bitcoin wallet owned by DIETRICH, and held in the Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com exchange, was identified and reviewed. The Bitcoin wallet identified as **Subject Wallet 1**. **Subject Wallet 1** was first observed on the Bitcoin blockchain on June 22, 2022. There have been 56 inbound and 56 outbound transfers. The inbound transfers totaled $132,189. The outbound transfers totaled $133,342. A review of the inbound transactions showed inbound transfers originating in the ChipMixer, CryptoMixer, and Wasabi cryptocurrency tumblers (see paragraph 32 for details). Inbound transfers were also observed with funds originating from known PhartmaHGH.net payment acceptance Bitcoin wallets. This wallet was also involved in multiple transfer chains where other GILBERT DTO members received funds.

54. A Bitcoin wallet owned by OLIVARRIA and held in the Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com exchange, was identified and reviewed. The Bitcoin wallet was identified as **Subject Wallet 2**. **Subject Wallet 2** was first observed on the bitcoin blockchain on May 9, 2021. This wallet has had 70 inbound and 70 outbound transactions. The inbound transfers totaled $45,018. The outbound transaction totaled $48,753. A review of the inbound transaction showed funds originating from the Wasabi and ChipMixer cryptocurrency tumblers (see paragraph 32 for details). Transfers were also observed from un-hosted wallets associated to transfers to other GILBERT DTO members. Inbound transfers were observed with the funds originating from known PharmaHGH.net payment acceptance wallets. OLIVARRIA was observed shipping parcels later found to contain steroids and was observed meeting with GILBERT on multiple occasions. OLIVARRIA was also observed receiving parcels from GILBERT later found to contain steroids.

55. A Bitcoin wallet owned by JIMENEZ and held in the Foris Dax Inc**,** Foris Inc**.** and Foris Services, Inc., dba Crypto.com exchange, was identified and reviewed. The Bitcoin wallet was identified as **Subject Wallet 3**. **Subject Wallet 3** was first observed on the bitcoin blockchain on September 21, 2021. This wallet has a total 33 inbound and 33 outbound transactions. The inbound transfers total $40,063. The outbound transfers total $42,341. A review of the inbound transaction showed funds originating from the Wasabi and ChipMixer cryptocurrency tumblers (see paragraph 32 for details). Transfers were also observed from un-hosted wallets associated to transfers to other GILBERT DTO members. Inbound transfers were observed with the funds originating

from known PharmaHGH.net payment acceptance wallets. In September 2024, GILBERT was observed shipping a parcel to JIMENEZ in Florida. The parcel was intercepted and through a field test indicated the parcel contained 310 grams of Oxazepam, a Schedule IV controlled substance. Multiple parcels have been shipped by GILBERT to JIMENEZ.

56. Throughout the course of this investigation, accounts were identified at First Interstate Bank owned by GILBERT. A Money Market account was identified with the account number 330410004321 (4321). This account was funded with the deposit of a $100,000 check from Patricia and Meredith Gilbert on November 22, 2022. These subjects have not been fully identified. On December 1, 2022, a $68,420.58 check was written to BMW of Tucson. This check was for the purpose of purchasing a BMW. On December 2, 2022, there was a "MISCELLANEOUS DEBIT" of $10,000 for this account. On December 6, 2022, there was an outgoing wire to Capetown Diamond Corp. for $12,500. The balance for this account at the end of December 2022 was $5,063.16. The debits listed for December 2022 totaled $94,945.58. In February 2022, deposits began being made from Coinbase.com. These deposits matched the transfers from GILBERT's now closed Coinbase wallet 3CGDo9m. Bank documents show the total deposits to this account from Coinbase to be $313,222.78 (It should be noted the discrepancy in the numbers seen in the Coinbase documents and the banks documents is likely due to the way Coinbase titles some of its withdrawals). The only deposits to this account not from Coinbase were the initial check and a $10,000 deposit in June of 2023. Records show this account as "Force Closed Account per Financial Crimes Risk

Mgmt" on January 29, 2024. A checking account was also identified for GILBERT at First Interstate. The account number for this account was 8002409932505 (2505). This account was funded by a $300.00 deposit on November 21, 2023. With the exception of the initial $300 deposit and a refund of $231.29 from PayPal all of the deposits into this account came by way of transfer from account 4321 detailed above. A payment was observed from this account to "ROLEX BY TOU HONOLULU HI" on May 1, 2023, in the amount of $26,597.01. A payment was observed to "LONDON JEWELERS SOUTH HAMPTON NY" on May 1, 2023, in the amount of $16,945.00. A payment was observed to "THE DIAMOND FAIR AIEA HI" on March 28, 2023, in the amount of $2,000.00. A payment was observed to "Sheffields DIAMO Oro Valley AZ" on September 13, 2023, in the amount of $7,000.00. A payment was observed to "OLIVER PEOPLES 8 HONOLULU HI" on January 9, 2024, for $648.17. A payment was observed to "LOUIS VUITTO HONOLULU HI" on January 9, 2023, for $706.96. Bank records show account 2505 was "Force Closed Account per Financial Crimes Risk Mgmt" on January 29, 2024. Again, the vast majority of funds entering into these cryptocurrency accounts were funds derived from sales by PharmaHGH.net for controlled substances (mostly steroids).

57. Wage inquiries through the Arizona Department of Economic Security were made for GILBERT, DIETRICH and OLIVARRIA. No wages were found for GILBERT. There is no evidence that GILBERT works at any legal or gainful employment. Wages were located for DIETRICH at Banner Health. For 2023 and the first quarter of 2024 DIETRICH made a total of $67,560. Wages were located for OLIVARRIA at Alaska

USA Federal Credit Union. For 2023 and the first quarter of 2024 OLIVARRIA made $89,484. The purchases of vehicles, travel, jewelry and other high-priced items were funded mostly by payments received through PharmaHGH.net which is in the business of selling steroids and other controlled substances. The amount of listed legal wages does not support the type of spending and lifestyle exhibited by GILBERT and DIETRICH.

CONCLUSION

58. Title 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it "determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a protective order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture." A protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that **Subject Wallets 1-3** will remain available for forfeiture, because there is a substantial risk that **Subject Wallets 1-3** will be withdrawn, moved, dissipated, or otherwise become unavailable unless immediate steps are taken to secure them at the time the requested seizures are executed. As forms of cryptocurrencies, **Subject Wallets 1-3** are inherently portable and fungible.

59. I respectfully request that the Court:

    a. Order the company hosting **Subject Wallet 1, Subject Wallet 2,** and **Subject Wallet 3** to send the full available balance of all accessible cryptocurrency through **Subject Wallet 1, Subject Wallet 2,** and **Subject Wallet 3** to a law enforcement-controlled wallet (when

applicable) or in the case of fiat currency, to law enforcement via check made payable to the U.S. Marshal's Office as directed or, if this is not possible,

b. Grant authorization for law enforcement agents to use the available username and/or login information, recovery seed (mnemonic phrase, root key, backup phrase, or private key) (if available) in their lawful possession to recover and reconstitute the **Subject Wallets 1-3** onto a different digital device and subsequently transfer all available cryptocurrency associated with **Subject Wallet 1, Subject Wallet 2,** and **Subject Wallet 3** to a wallet controlled by law enforcement.

I declare under penalty that the foregoing is true and correct to the best of my knowledge, information, and belief.

FURTHER, your affiant sayeth not.

ALEJANDRO URZUA

Digitally signed by ALEJANDRO URZUA
Date: 2025.01.23 11:13:00 -07'00'

Alejandro Urzua
Special Agent
Drug Enforcement Administration

Subscribed and sworn to telephonically this 23rd of January, 2025.

Hon. Lynnette C. Kimmins
United States Magistrate Judge